JOURNAL OF NUMBER THEORY 1, 231–234 (1969)

Über die Klassenzahl des Körpers $P(\sqrt{-2p})$ mit einer Primzahl $p \neq 2$

HELMUT HASSE†

University of Hamburg, Hamburg, Germany

Communicated October 21, 1968

P. Barrucand and H. Cohn recently gave a new criterion for the divisibility by 2^3 of the class number of $\sqrt{-p}$ ($p \equiv 1 \bmod 2^3$). Here a similar criterion is given for the class number of $\sqrt{-2p}$ ($p \neq 2$), viz., that it is divisible by 2^3 iff $p = \pm 1 \bmod 2^3$ and in an integral representation $-2p = u^2 - 2v^2$ with $v>0$ holds $v \equiv 1, -(1+2^2)$ or $1, -1 \bmod 2^3$ according to $p \equiv +1$ or $-1 \bmod 2^3$.

0. In einer kürzlich erschienen Arbeit [*1*] haben P. Barrucand und H. Cohn unter anderem bewiesen, dass die Klassenzahl des imaginär-quadratischen Zahlkörpers von $\sqrt{-p}$ mit einer Primzahl $p \equiv 1 \bmod 2^3$ genau dann durch 2^3 teilbar ist, wenn in einer und damit jeder ganzzahligen Darstellung

$$-p = u^2 - 2v^2 \quad \textit{mit } v > 0 \quad \textit{gilt } v \equiv 1 \bmod 2^2,$$

oder auch genau dann, wenn in der ganzzahligen Darstellung

$$p = x^2 + 2y^2 \quad \textit{gilt } y \equiv 0 \bmod 2^2.$$

In einer daran anknüpfenden Arbeit [*2*] habe ich diese Kriterien in einfacher, naturgemässer Weise aus der Geschlechtertheorie der quadratischen Zahlkörper hergeleitet.

Die dort betrachteten imaginär-quadratischen Zahlkörper sind solche, deren Diskriminante ausser einer einzigen Primzahl $p \neq 2$ nur noch die Primzahl 2 enthält, so dass nach der Geschlechertheorie ihre 2-Klassengruppe den 2-Rang 1 hat, d.h. zyklisch ist. Es gibt noch eine weitere Serie solcher imaginär-quadratischer Zahlkörper, nämlich die von $\sqrt{-2p}$ mit einer Primzahl $p \neq 2$ erzeugten. In der vorliegenden Arbeit leite ich für sie ein analoges Kriterium her, dass nämlich hier die Klassenzahl zunächst

† Author's address for academic year 1968–69: Department of Mathematics, University of Hawaii, Honolulu, Hawaii 96822.

genau dann durch 2^2 teilbar ist, wenn $p \equiv \pm 1 \bmod 2^3$ ist—das wurde vor längerer Zeit bereits von Rédei und Reichardt festgestellt [3], [4] —, und wenn diese Bedingung erfüllt ist, genau dann sogar durch 2^3 teilbar ist, wenn zudem in einer und damit jeder ganzzahligen Darstellung

$-2p = u^2 - 2v^2$ *mit* $v > 0$ *gilt*

$$\begin{Bmatrix} v \equiv 1, \ -(1+2^2) \bmod 2^3, \textit{falls } p \equiv +1 \bmod 2^3 \\ v \equiv 1, \ -1 \qquad\quad \bmod 2^3, \textit{falls } p \equiv -1 \bmod 2^3 \end{Bmatrix}.$$

Ein damit äquivalentes Kriterium, das sich wie in [1] auf eine *definite* quadratische Form stützt, konnte ich allerdings hier nicht feststellen†.

1. Analog zu [1] sei hier

$$K = P(\sqrt{-2p}) \qquad (p \neq 2 \text{ Primzahl})$$

der betrachtete imaginär-quadratische Zahlkörper. Seine Diskriminante ist $d = -2^3 p$, ihre Primteileranzahl $t = 2$, und diese beiden Primteiler sind in K verzweigt:

$$2 \cong \mathfrak{z}^2 \quad \textit{mit} \quad N(\mathfrak{z}) = 2, \qquad p \cong \mathfrak{p}^2 \quad \textit{mit} \quad N(\mathfrak{p}) = p.$$

Die Divisorenklassengruppe D von K hat, wie schon bemerkt, den 2-Rang $t-1 = 1$, d.h. es ist

$$[D : D^2] = 2^1,$$

so dass die 2-Klassengruppe zyklisch ist. Für die Klassenzahl h von K gilt jedenfalls

$$2^1 | h.$$

2. Die einzige 2-Klasse der Ordnung 2 von K wird etwa durch den Verzweigungsprimdivisor $\mathfrak{z}$ repräsentiert; denn einerseits hat man $\mathfrak{z}^2 \cong 2 \sim 1$, andererseits ist $\mathfrak{z} \nsim 1$, da 2 nicht ganzzahlig als Norm $a^2 + 2pb^2$ einer Zahl aus K darstellbar ist. Demnach ist

$$2^2 | h \Leftrightarrow \mathfrak{z} \in D^2.$$

Nun ist D^2 das Hauptgeschlecht von K. Die Divisoren $\mathfrak{a}$ aus D^2 sind durch die beiden Geschlechtscharakterwerte

$$\left(\frac{-2p,\, N(\mathfrak{a})}{2}\right) = 1, \qquad \left(\frac{-2p,\, N(\mathfrak{a})}{p}\right) = 1$$

gekennzeichnet. Auf Grund der zwischen ihnen bestehenden Abhängigkeit (Produktformel für das Normsymbol, quadratisches Reziprozitätsgesetz)

† Einer freundlichen Mitteilung von Barrucand entnehme ich, dass sich im Falle $p \equiv 1 \bmod 2^3$ aus (recht heterogenen) Ergebnissen von Glaisher [5] leicht ain solches Kriterium gewinnen lässt, nämlich $y \equiv 0 \bmod 2$, *wo* $p = x^2 + 2^2y^2$, und dass sich im Falle $p \equiv -1 \bmod 2^3$ mein Kriterium zu $p \equiv -1 \bmod 2^4$ vereinfachen lasst.

genügt es, etwa den ersteren in Betracht zu ziehen. Für den Verzweigungsdivisor $\mathfrak{z}$ findet sich

$$\left(\frac{-2p,\, N(\mathfrak{z})}{2}\right) = \left(\frac{-2p,\, 2}{2}\right) = \left(\frac{p,\, 2}{2}\right) = \begin{Bmatrix} +1 \textit{ für } p \equiv \pm 1 \bmod 2^3 \\ -1 \textit{ für } p \not\equiv \pm 1 \bmod 2^3 \end{Bmatrix}.$$

Demnach ist

$$\mathfrak{z} \in D^2 \Leftrightarrow p \equiv \pm 1 \bmod 2^3.$$

Zusammengenommen ergibt sich so:

$$2^2 | h \Leftrightarrow p \equiv \pm 1 \bmod 2^3.$$

3. Sei weiterhin $p \equiv \pm 1 \bmod 2^3$ vorausgesetzt. Dann ist die Relation

$$\mathfrak{z} \sim \mathfrak{a}^2 \quad \text{oder also} \quad \mathfrak{z}\mathfrak{a}^2 \sim 1$$

durch einen Divisor $\mathfrak{a}$ von K lösbar. Dieser repräsentiert eine der beiden 2-Klassen der Ordnung 2^2 von K. Demnach hat man

$$2^3 | h \Leftrightarrow \mathfrak{a} \in D^2.$$

Um einen solchen Repräsentanten $\mathfrak{a}$ zu finden, nehme man irgendeine ganzzahlige Darstellung

$$-2p = u^2 - 2v^2 \quad \textit{mit} \quad v > 0,$$

vorhanden weil $(2/p) = 1$ ist und $P(\sqrt{-2})$ die Klassenzahl 1 und Grundeinheitsnorm -1 hat. In der Form

$$u^2 + 2p = 2v^2$$

geschrieben ergibt diese Darstellung eine Zahl

$$\omega = u + \sqrt{-2p} \quad \textit{mit} \quad N(\omega) = 2v^2$$

aus K. Diese Zahl ω ist primitiv, so dass der grösste gemeinsame Teiler $(\omega, \bar{\omega}) | \mathfrak{z}\mathfrak{p}$. Wegen $2 | N(\omega)$ ist $\mathfrak{z} | \omega$, und wegen $p \nmid N(\omega)$ ist $\mathfrak{p} \nmid \omega$. Daher hat man $(\omega, \bar{\omega}) = \mathfrak{z}$. Nach Wegdivision von $\mathfrak{z}$ wird

$$\left(\frac{\omega}{\mathfrak{z}}, \frac{\bar{\omega}}{\mathfrak{z}}\right) = 1 \quad \textit{mit} \quad N\left(\frac{\omega}{\mathfrak{z}}\right) = v^2.$$

Daraus folgt

$$\frac{\omega}{\mathfrak{z}} = \mathfrak{a}^2 \quad \text{oder also} \quad \omega \cong \mathfrak{z}\mathfrak{a}^2 \quad \text{und somit} \quad \mathfrak{z}\mathfrak{a}^2 \sim 1$$

mit einem Divisor $\mathfrak{a}$ von K, wie verlangt.

Der so konstruierte Divisor $\mathfrak{a}$ hat $N(\mathfrak{a}) = v$; man beachte die Normierung $v > 0$. Damit berechnet sich der obige Geschlechtscharakter für

$\mathfrak{a}$ wie folgt:

$$\left(\frac{-2p,\, N(\mathfrak{a})}{2}\right) = \left(\frac{-2p,\, v}{2}\right) =$$
$$\begin{Bmatrix} \left(\frac{-2,\, v}{2}\right) = (-1)^{\frac{v-1}{2}+\frac{v^*-1}{2^2}} & \textit{für } p \equiv +1 \bmod 2^3 \\ \left(\frac{2,\, v}{2}\right) = (-1)^{\frac{v^*-1}{2^2}} & \textit{für } p \equiv -1 \bmod 2^3 \end{Bmatrix}$$

mit $v^* = (-1)^{(v-1)/2}v$; man beachte, dass wegen $p \equiv \pm 1 \bmod 2^3$ notwendig $v \equiv 1 \bmod 2$ ist. Demnach ist

$$\mathfrak{a} \in D^2 \Leftrightarrow \begin{Bmatrix} v \equiv 1,\ -(1+2^2) \bmod 2^3 & \textit{für } p \equiv +1 \bmod 2^3 \\ v \equiv 1,\ -1 \qquad \bmod 2^3 & \textit{für } p \equiv -1 \bmod 2^3 \end{Bmatrix}.$$

Zusammengenommen ergibt sich so:

$$2^3 | h \Leftrightarrow \begin{Bmatrix} v \equiv 1,\ -(1+2^2) \bmod 2^3 & \textit{für } p \equiv +1 \bmod 2^3 \\ v \equiv 1,\ -1 \qquad \bmod 2^3 & \textit{für } p \equiv -1 \bmod 2^3 \end{Bmatrix}.$$

wie eingangs behauptet.

Dass die im Ergebnis auftretende Alternative für $v \bmod 2^3$ unabhängig von der gewählten Darstellung $-2p = u^2 - 2v^2$ with $v > 0$ ist, folgt implizit aus dem Ergebnis selbst, oder auch explizit durch Multiplikation von $u + v\sqrt{2}$ mit der total-positiven Grundeinheit $3 + 2\sqrt{2}$ unter Beachtung von $u \equiv 0$ oder $2 \bmod 2^2$ je nachdem $p \equiv +1$ oder $-1 \bmod 2^3$.

LITERATURVERZEICHNIS

1. BARRUCAND, P., UND COHN, H. Notes on primes of type $x^2 + 32y^2$, class number and residuacity. *J. Reine Angew. Math.* **237** (1969).

2. HASSE, H. Über die Klassenzahl des Körpers $P(\sqrt{-p})$ mit einer Primzahl $p \equiv 1 \bmod 2^3$. *Aequationes Math.* 254–258.

3. REDEI, L., UND REICHARDT, H. Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers. *J. Reine Angew. Math.* **170** (1934), 69–74. Dieser Arbeit ging eine Mitteilung (ungarisch) von Rédei allein voraus: *Math. Naturwiss. Anz. Ungar. Akad. Wiss.* **48** (1931), 683–707.

4. REICHARDT, H. Zur Struktur der aboluten Idealklassengruppe im quadratischen Zahlkörper. Ebendort 75–82.

5. GLAISHER, J. W. L. On the expression for the number of classes of a negative determinant, and on the number of positives in the octants of P. *Quart. J. Pure Appl. Math.* **34** (1903), 178–204.